PTO/SB/08A (Substitute for form 1449/PTO)	Attorney Docket No.:	*004-9388*
	Application No.:	*10/626,420*
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	First Named Inventor:	*Sheueling Chang Shantz*
(Use several sheets if necessary)	Filing Date:	*July 24, 2003*
	Group Art Unit:	*2131*
	Examiner Name:	*Ayaz R. Sheikh*
	Date Submitted:	*December 7, 2004*

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
CJ		US-5,121,431	06-09-1992	Wiener	
CJ		US-6,633,896 B1	10-14-2003	Moore et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5](if known)	Publication Date MM-DD-YYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		EP 0 247 383 A3	12-02-1987	Hasebe		

Examiner Signature	/Carlton Johnson/	Date Considered	01/22/2007

PTO/SB/08B (Substitute for form 1449/PTO)		Attorney Docket No.:	004-9388
		Application No.:	10/626,420
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		First Named Inventor:	Sheueling Chang Shantz
(Use several sheets if necessary)		Filing Date:	July 24, 2003
		Group Art Unit:	2131
		Examiner Name:	Ayaz R. Sheikh
		Date Submitted:	December 7, 2004

NON PATENT LITERATURE DOCUMENTS

Examiner Initial*	Cite No.[1]	Include name of author (in CAPITAL LETTERS), title of article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
CJ		Yvonne Hitchcock, et al., "Implementing an efficient elliptic curve cryptosystem over GF(p) on a smart card," ANZIAM J. 44(E), April 2003, pp. C354-C377.	
CJ		National Institute of Standards and Technology, "Recommended Elliptic Curves for Federal Government Use," August 1999, 43 pages.	
CJ		Hasegawa, Toshio, et al., "A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit Microcomputer," In *Public Key Cryptography* PKC '98, vol. 1431 of *Lecture Notes in Computer Science*, pages 182-194.	

Examiner Signature	/Carlton Johnson/	Date Considered	01/22/2007

U.S. Department of Commerce, Patent and Trademark Office	Attorney Docket No.:	*004-9388*
	Application No.:	*10/626,420*
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s):	*Sheueling Chang Shantz et al.*
(Use several sheets if necessary)	Filing Date:	*July 24, 2003*
	Group Art Unit:	*3621*
	Date Submitted:	*July 1, 2004*

NON PATENT LITERATURE DOCUMENTS

*Examiner Initial	Cite No.	(Including name of author in capital letters, title of article, title of item, date, pertinent pages, volume-issue number(s), publisher, city and/or country where published.)
CJ	AA	Intel® Itanium™ Processor, "High Performance On Security Algorithms (RSA Decryption Kernel)," Intel Corporation, 2001, pp. 1-8.
CJ	AB	Intel®, "Intel® Itanium™ Architecture Software Developer's Manual, Volume 1: Application Architecture," Revision 2.1, October, 2002, 2 pages.
CJ	AC	Großschädl, Johann, "Instruction Set Extension for Long Integer Modulo Arithmetic on RISC-Based Smart Cards," Proceedings of the 14th Symposium on Computer Architecture and High Performance Computing, 2002, 7 pages.
CJ	AD	Koç, Cetin Kaya, "High-Speed RSA Implementation," Version 2.0, RSA Laboratories, November, 1994, pp. i-70.
CJ	AE	Shantz, Sheueling Chang, "From Euclid's GCD to Montgomery Multiplication to the Great Divide," Sun Microsystems, June 2001, pp. 1-10.
CJ	AF	Standards for Efficient Cryptography, "SEC 2: Recommended Elliptic Curve Domain Parameters," Certicom Research, September 20, 2000, pp. i-45.
CJ	AG	Woodbury, A.D.; Bailey, Daniel V., Paar, Christof, "Elliptic Curve Cryptography on Smart Cards Without Coprocessors," The Fourth Smart Card Research and Advanced Applications (CARDIS2000) Conference, Bristok, UK, pp. 71-92.
CJ	AH	H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates", in K. Ohta and D. Pei, editors, Advances in Cryptology ASIACRYPT 98, pp. 51-65, Springer Verlag, 1998, LNCS 1514
CJ	AI	D. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms." In H. Krawczyk, editor, Advances in Cryptography – CRYPTO '98, volume LNCS 1462, pages 472-485. Springer-Verlag, 1998. http://citeseer.ist.psu.edu/article/bailey98optimal.html, 14 pages.
CJ	AJ	H. Pietiläinen, "Elliptic Curve Cryptography on Smart Cards," Master's Thesis, Helsinki University of Technology, Oct. 12, 2000, pp. i-81.
CJ	AK	F. Morain and J. Olivos, "Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains," Rapport de Recherche 983, INRIA, France, March 1989, http://citeseer.ist.psu.edu/morain90speeding.html, pp. 119-130.
	AL	
	AM	
	AN	
	AO	
	AP	
	AQ	

Examiner /Carlton Johnson/	Date Considered 02/24/2007

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.